SECTION XVI. COMSEC INSECURITY REPORTING REQUIREMENTS

112. General. To be successful, the National COMSEC Insecurity Reporting System must receive an uninhibited flow of information relating to a clear understanding of the circumstances surrounding an insecurity. Thus, users of COMSEC material must be encouraged to report COMSEC insecurities promptly. Adherence to the following guidelines will ensure the success of the system.

a. Every person who will deal in any way with COMSEC material must understand his or her responsibilities for immediately reporting insecurities to the FSO or his designated representative. These officials must report COMSEC insecurities as prescribed in this Section. Insecurity reports must be submitted promptly and not be delayed in administrative channels.

b. Individuals will not be disciplined for reporting a COMSEC insecurity. Corrective measures are most productive when aimed at the national doctrine or the organizational policy or procedure which allowed or contributed to the insecurity. Disciplinary action should normally be taken only against the perpetrator or perpetrators of grossly negligent or willful acts which jeopardize the security of COMSEC material.

113. Types of COMSEC Insecurities. COMSEC insecurities fall into three categories, as noted below. Included under each category are representative types of reportable insecurities. Additional reportable insecurities which are peculiar to a given cryptosystem are normally listed in the operating instructions, and maintenance manual(s) for that cryptosystem.

a. Cryptographic Insecurities.

(1) Use of COMSEC key which is compromised, superseded, defective, previously used and not authorized for reuse, or in any way incorrect for the cryptoperiod or application in which it is used; e.g.:

(a) Unauthorized use of any key for other than its intended purpose.

(b) Use of key which was produced locally without the authorization of the Director, NSA. 1/

(c) Unauthorized extension of a cryptoperiod.

(d) Premature use of key.

NOTE : Failure to zeroize a common-fill device within the required time must be reported as a physical insecurity.

(2) Use of a cryptosystem or a cryptosystem operating practice or maintenance practice which is not approved by NSA; e.g. ,

---

1/ DIRNSA AUTHORIZATION TO GENERATE KEY IN THE FIELD IS IMPLICIT IN THE PUBLICATION OF OPERATING INSTRUCTIONS FOR CRYPTOSYSTEMS WHICH POSSESS THAT CAPABILITY.

(a) Operational use of a COMSEC equipment without completion of a required alarm-check test or after failure of a required alarm-check test.

(b) Actual or attempted maintenance of a COMSEC equipment by unqualified personnel.

(3) Use of COMSEC equipment having defective cryptographic logic circuitry; e.g.:

(a) Plaintext transmission resulting from a COMSEC equipment failure or malfunction.

(b) Any transmission during or after an uncorrected failure, that may cause improper operation of a COMSEC equipment.

(4) Discussions via nonsecured telecommunications of the details of a crypto-equipment failure or malfunction.

(5) Tampering with, or unauthorized modifications of, a COMSEC equipment or system.

(6) Compromising emanations from a COMSEC equipment.

(7) Any other occurrence which may have resulted in a cryptographic insecurity.

b. Personnel Insecurities.

(1) Known or suspected defection, espionage, hostile cognizant agent activity, treason, sabotage, or capture by an enemy of persons who have detailed knowledge of cryptographic logic or uncontrolled access to keying material.

(2) Theft of COMSEC material.

(3) Deliberate falsification of COMSEC records.

(4) Unauthorized disclosure of information concerning COMSEC material or attempts by unauthorized persons to effect such disclosure.

c. Physical Insecurities.

(1) The physical loss of COMSEC material, including a portion(s) thereof (e.g., a CCI equipment or a classified page from a crypto-equipment maintenance manual).

(2) COMSEC material discovered outside of required COMSEC accountability or physical control; e.g.:

(a) COMSEC material reflected on a destruction report as having been properly destroyed and witnessed, but found not to have been destroyed.

(b) COMSEC material left unsecured and unattended where unauthorized persons could have had access.

(3) COMSEC material improperly packaged, shipped, or destroyed; e.g.:

(a) COMSEC material received in a damaged package.

(b) Destruction of COMSEC material by other than authorized means or COMSEC material not completely destroyed and left unattended.

(4) COMSEC material received in a package which shows evidence of tampering, or known or suspected tampering with COMSEC material at any time.

(5) Unauthorized access to COMSEC material.

(6) Failure to zeroize a common fill device within the required time.

(7) Premature opening of a sealed package of keying material.

(8) Unexplained loose keycards in a package having a wide-band seal.

(9) Unauthorized copying, reproducing, or photographing of COMSEC material.

(lo) A clandestine intercept or recording device discovered in or near a COMSEC facility.

(11) Any other incident which jeopardizes the physical security of COMSEC material.

114. Reporting Insecurities. When reporting insecurities, the contractor must make an immediate telephonic notification to the DIS CSO and NSA of any incident or violation of the security requirements specified in this Supplement irrespective of the contractor's judgement as to whether or not an insecurity or possible insecurity occurred. Where secure means of transmission are available, the initial report will provide all the details known at that time. Where the notification is made over an unsecure-mode, the insecurity report should be limited to minimum essential information. During normal duty hours (0730-1730 EST), notification to NSA will be made to the COMSEC Insecurity Branch (S213) on (301) 688-6010 or 6948. After normal duty hours and on weekends and holidays, the notification will be made to the Senior Information Security Coordinator on (301) 688-7003. The initial telephonic report must be followed up with a letter report, classified according to its contents, and securely forwarded. Unclassified reports will be marked For Official Use Only.

115. Types of Reports.

a. Initial Report. An initial written report is required for each detected COMSEC insecurity. If all of the facts regarding the incident are included in the initial report, it may also serve as the final report,

provided it contains all information required by paragraph 115d, below. In such cases, paragraph 6 of the initial report will include a request that the report be accepted as a final report.

b. Amplifying Report. Whenever significant, new information concerning a reported incident is discovered, an amplifying report is required. An amplifying report may also serve as the final report, provided it contains all information required by paragraph 115d, below. In such cases, paragraph 6 of the amplifying report must include a request that the report be accepted as a final report.

c. Interim Report. If a final report is not submitted within 30 days after the initial report or the last amplifying report, an interim report will be submitted every 30 days until the final report is submitted. The interim report will advise of the status of an inquiry or investigation, or other reason for delay of the final report.

d. Final Report. A final report is required for each reported COMSEC insecurity unless the initial or an amplifying report also served as the final report. The final report must include a summary of the results of all inquiries and investigations, and it will identify corrective measures taken or planned to minimize the possibility of recurrence.

116. Format and Content of Insecurity Letter Reports. Format and content requirements for insecurity letter reports are set forth below. Where subsequent reports would merely duplicate information previously reported, the information need not be repeated. Instead, reference will be made to the previous report which contains the information.

a. Subject. The subject of the report will consist only the words "COMSEC Insecurity."

b. References. The report must include reference(s), as applicable, to:

(1) The paragraph number of the operating, maintenance, or Agency or Department instruction or this supplement in which the reported insecurity is listed, or the statement: "Formal reporting requirements cannot be identified at this time."

(2) Previously forwarded, related insecurity reports and other correspondence identified sufficiently to permit location (e.g. , date, time, office symbol, etc.).

c. Material Involved. Paragraph 1 of the report must identify the COMSEC material involved. Include the short title (including edition designator, modification suffix letter, and MATSYM or system designator, if applicable) ; register, accounting and serial number (as applicable) of Accounting Legend Code 1 and 3 material (all other material by quantity); specific cards, tape segments, tables, and days if not a complete document; a description of the material or equipment involved; and whether equipment was keyed or unkeyed. Where the insecurity involves keying material, identify the controlling authority for each short title.

d. Personnel Involved. For personnel insecurities only, paragraph 2 of the report must identify the individual(s) who caused, or was otherwise responsible for, the insecurity. Include for each individual: name, citizenship, duty position, and level of security clearance held. For all other COMSEC insecurities, provide only the duty position, the level of security clearance, if known, and the nationality of the individual(s) involved.

e. Location of Incident. Paragraph 3 of the report must identify the location of the incident, the responsible facility, and its COMSEC account numb er.

f. Circumstances of Incident. Paragraph 4 of the report must identify the circumstances surrounding the insecurity. Give a chronological account of the events which led to the discovery of the insecurity and, when known, sufficient details to give a clear picture of how the insecurity occurred. The chronology must include all relevant dates, times of day, frequencies of events, etc. Include a description of the security measures in effect at the location, and estimate the possibility of unauthorized personnel having access to the COMSEC material involved. Paragraph 4 of amplifying report may also be used to report significant new information not included in other paragraphs of the report.

g. Additional Reporting Requirements. Paragraph 5 of the report will include any additional reporting that may be required. The following subparagraphs list the reporting requirements for specific incidents or items.

(1) Improper use of Keying Material or Use of Improper Operating Procedures.

(a) A description of the associated communications activity (e.g., online/offline, simplex/half-duplex/full-duplex, point-to-point/netted operations).

(b) The operating mode of the crypto-equipment (e.g., clock start, message indicator, traffic flow security).

(c) The general type of traffic involved, if any (SI/SAO, voice, data).

(2) Operational Use of Malfunctioning COMSEC Equipment.

(a) The symptoms of the malfunction.

(b) The likelihood that the malfunction was deliberately induced. If so, see subparagraph (8) , below.

(c) The amount and type of traffic involved, if any.

(3) Known or Suspected Defection, Espionage, Hostile Cognizant Agent Activity, Treason, Sabotage, or Capture.

(a) The individual's general background in COMSEC and the extent of his/her knowledge of crypto-principles.

(b) List the cryptosystems to which the individual had current access and state whether the access was to cryptographic logic and/or key. (For logic, state whether access was to full or limited maintenance manuals, and for key state the short titles and edition identifiers involved.)

(4) Loss of COMSEC Material.

(a) The actions being taken to locate the material.

(b) The possibility of access by unauthorized persons.

(c) The possibility of removal of material by authorized or unauthorized persons.

(d) The methods of disposal of all classified and unclassified waste and the possibility of loss by those methods.

(5) COMSEC Material Discovered Outside of Required COMSEC Accountability or Physical Control.

(a) The action which caused accountability or physical control to be restored.

(b) The possibility of access, surreptitious or otherwise, by unauthorized persons.

(c) The estimated length of time the material was unsecured.

(6) COMSEC Material Received in a Damaged Package.

(a) The means of transmittal (when the damage occurred in transit).

(b) A description of how the material was stored (when the damage occurred in storage).

NOTE : Ensure all packaging containers, wrappers, etc., are retained until destruction is authorized or directed.

(7) COMSEC Material Received in a Package that Shows Evidence of Tampering, or known or Suspected Tampering at Any Time.

(a) A description of the evidence of known or suspected tampering.

(b) The means of transmittal (when the suspected tampering occurred in transit).

(c) A description of how the material was stored (when the suspected tampering occurred in storage).

NOTE : When tampering is known or suspected, immediately seal the package and/or material in a plastic (or any other) wrapper and place it in the most

secure, limited-access storage available. Handle the package and/or material as little as possible until instructions are received from NSA. Take no action that would jeopardize potential evidence.

(8) Unauthorized Copying, Reproduction, or Photographing.

(a) A complete identification of the equipment or material copied or photographed.

(b) The reason for reproduction and how the reproduced material was controlled.

(c) Whether espionage is indicated or suspected. If so, see subparagraph (3), above.

(d) The degree to which details of equipment internals, keying material, or documents were copied or photographed.

NOTE : A copy of each photograph or other reproduction must be included with the insecurity letter report.

(9) Unauthorized Modification or Maintenance of a COMSEC Equipment, or Discovery of a Clandestine Intercept or Recording Device in or Near a COMSEC Facility.

(a) A description of the modification, or device; its installation and symptoms; and the host equipment involved.

(b) An estimate of how long the item may have been in place.

(c) An estimate of the classified information/traffic jeopardized.

NOTE : Hold information concerning these types of insecurities on a strict need-to-know basis. The equipment or devices should not be used or otherwise disturbed until further instructions are received from NSA. Where a clandestine intercept or recording device is suspected, do not speak about it in the area of the device. Nothing should be done that would possibly alert the COMSEC exploiter, except on instructions from NSA.

h. Possibility of Compromise. Paragraph 6 of the report must state which of the following opinions is applicable: compromise certain, compromise possible, compromise improbable; and will include the basis for the opinion. Where an initial or amplifying report is to also serve as the final report, paragraph 6 must include a request that the report be accepted as a final report.

i. Point of Contact. Paragraph 7 of the report will include the name, commercial telephone number, and, if available, secure telephone number of an individual who is prepared to respond to questions from the evaluating authority.

THIS PAGE INTENTIONALLY LEFT BLANK